Regional Insurance Group Network Redesign Report

Regional Insurance Group's original network architecture relied on a single firewall at the perimter of the network, and lacked internal network segmentation. The design created several security risks because sensitive systems and basic departmental resources were being housed on the same network segment. The new and improved, redesigned network improves the organization's security position by introducing network segmentation between departments, layered firewall protection, and a new system for authentication. These improvements follow network design principles such as defense in depth, diversity of defense, segmentation and least privilege access.

Segmentation

Logical network separation between the accounting and sales departments was implemented using Virtual Local Area Networks or VLANs. VLANs allow multiple "logical" networks to exist on the same physical network. This keeps traffic isolated between departments.

The Accounting department is assigned VLAN 10, while the Sales department is assigned VLAN 20. Each department's workstations connect to switch ports configured for their respective VLAN. This prevents direct communication between departments.

A switch performs inter-VLAN routing when communication between departments or networks is needed. Firewall rules also further restrict access to any sensitive resources, ensuring that only authroized systems have the ability to communicate across VLANs. This design is intentional to prevent lateral movement within the network which protects each individual VLAN network from being compromised if one of them becomes compromised.

Firewall Selection and Placement need sources

The redesigned network uses a layered firewall design to protect different parts of the network infrastructure. The perimeter firewall remains in use. A perimeter firewall is not a bad thing, it was just not enough for this organization. The perimeter firewall is a pfsense firewall. This firewall supports packet filtering, network address translation, VPNs, and intrusion detection features.

A second firewall has been introduced between the DMZ and the internet network in order to restrict communication between the publicly available services within the DMZ and the private systems within the internal network. This segmentation firewall ensures that only specific, and necessary traffic is allowed to reach and access internal systems. For this firewall I decided to go with an OPNsense firewall. This firewall option provides all of the same great features but introduces the practice of diversity of defense

In addition to our network firewalls, each Windows system uses Windows Defender Firewall. This provides one more security layer which also controls incoming and outgoing traffic, but at

the device level. This multied layer approach follows defense in depth practices when building a network.

DMZ Implementation

A demilitarized zone or a DMZ has been implemented in order to isolate publicly accessible systems from the local network. The organization's public facing web server which houses the customer portal is placed within this DMZ network which is now a segment of the original network.

The DMZ network has been connected to the perimeter firewall and completely separated from the internal network thanks to the new internal firewall. Only specific services required for customer access like HTTP and HTTPS traffic are allowed into the DMZ. Communication is also strictly controlled between the DMZ and the internal systems through the firewall rules.

The implementation of a DMZ provides security by limiting the exposure of internal systems to external attacks and threats. If the public facing web server were to become compromised, attackers would be stuck inside the DMZ and unable to directly access any of the internal systems including the sensitive ones. This design follows the best practice for protecting networks with a LAN to WAN domain.

Network Authentication need sources

The new redesigned network now includes authentication services that secure access to internal resources. Most of the systems are windows so the authentication services are provided by and managed with Microsoft Active Directory running on a windows server.

An active directory domain controller was placed within a dedicated authentication VLAN so that it was completely isolated. When users log in to their workstatuions, their credentials are verified by the domain controller before access to network resources like any servers or files can be granted.

In addition to active directory, strong password policies, account lockout policies and role based access rules are also implemented to stregthen physical security. The principle of least privilege has also been enforced by allowing users access to only what they need for their job description.

Summary of Network Configuration Changes

Several major changes were made to the network in order to strengthen the security of the system before changes to how Regional Insurance Group runs their business can actually work. First, VLAN segmentation was introduced which logically divided the accounting and sales departments as well as isolated a server VLAN and a new authentication VLAN.

Second, an additional firewall was deployed which provided an internal and external network segmentation and improved overall security for all internal systems.

Third, a DMZ network was implemented which isolated the public web server from all of the internal systems which reduces exposure threats to the internal network. Last, authentication services were deployed using Active Directpory which prodives identity management and access control.

Together all of these changes become a huge improvement for Regional Insurance Group, and sets them up for expansion and success as a more secure and flexible company.

References

OPNsense. (n.d.). OPNsense open source firewall and routing platform. https://opnsense.org/

pfSense. (n.d.). pfSense open source firewall. https://www.pfsense.org/

Active Directory Domain Services. (n.d.). Active Directory Domain Services overview. Microsoft. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview